ParsePort Security Standards VN06112023

1 ParsePort Information Security Standards.

1.1 ParsePort will maintain a comprehensive information security program ("ParsePort Security Program") which includes administrative, technical, and physical safeguards to protect Customer's data. ParsePort safeguards are maintained to appropriately protect Customer's data based on commercially reasonable and industry standard resources available to ParsePort and the type of the Customer's data. The ParsePort Security Program is designed to:

(a) Protect the availability, integrity and confidentiality of customer data;

(b) Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer's data;

(c) Protect against any unlawful unauthorized access, unlawful use, disclosure, alteration, or destruction by ParsePort of Customer's data; and

(d) Protect against any accidental loss, destruction, or damage to Customer's data.

1.2 ParsePort will also monitor, evaluate, and modify the ParsePort security program to ensure:

(a) Use of industry standard technology pertinent to the protection of Customer's data;

(b) Commercially reasonable updates to the Products and Services, ParsePort Security Program or ParsePort's systems, based on relevant changes in internal procedures for the protection of Customer's data, or as necessary to comply with applicable law; and

(c) ParsePort relevant internal changes to ParsePort's technical environment including third parties, outsourcing arrangements, infrastructure, and information systems.

2 Governance. ParsePort will maintain a governance program which includes:

2.1 Compliance with the baseline of security controls for a Software as a Service (SaaS) Cloud Service Provider

2.2 Policies and procedures based on the ISO 27001:2013 framework;

2.3 Data classification;

2.4 EU based datacenters for storage of Customer's data when in use;

2.5 Risk management; and

2.6 Third party security risk management.

3 Access Controls. ParsePort will maintain policies, procedures and logical controls designed to:

3.1 Limit access to ParsePort facilities and systems where those systems are limited to authorized persons;

3.2 Limit ParsePort employees' access to Customer's data by enforcing segregation of duties;

3.3 Protect from unauthorized access to Customer's data;

3.4 Remove or restrict ParsePort employees' access to Customer's data in a timely manner when access thereto is no longer required to perform Services, or upon Customer request;

3.5 Require multi-factor authentication through Federated Service for ParsePort access to Customer's data for the provision of Services; and.

3.6 Maintain a strong password policy (i.e., 12 character, alpha, special, numeric with two factor authentication).

4 Human Resource Security. ParsePort will maintain security and privacy policies and procedures for Human Resource including:

4.1 Performing pre-employment background screening commensurate with such employee's level of access to data, subject to applicable law;

4.2 Ensuring that all employees are bound by confidentiality obligations;

4.3 Annual security and privacy role-based training (including requirements of the ParsePort Security Program, the importance of security Customer’s data, and how to diagnose phishing attacks); and

4.4 Promoting a culture of security awareness through periodic training, phishing assessments, blogs, and programs which reward security best practices.

5 Physical and Environmental Security. ParsePort will maintain controls that are designed to protect from unauthorized access and against environmental hazards, including:

5.1 Controlled access to ParsePort facilities;

5.2 Inheritance of Physical and Environmental security controls from ISO27001:2013 compliant Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) CSPs.

5.3 Logging and monitoring of access and unauthorized access to ParsePort facilities and systems;

5.4 Camera monitoring of ParsePort facilities;

5.5 Temperature, fire protection, humidity monitoring of ParsePort facilities; and

5.6 Uninterrupted power supplies to ParsePort facilities to maintain normal working conditions in compliance with our Business Continuity Plan.

6 Secure Development Lifecycle. ParsePort will maintain policies and procedures which will assure that development is done with commercially reasonable security practices including:

6.1 Secure development policies;

6.2 Secure development training;

6.3 Configuring systems and network devices in accordance with ParsePort hardening guidelines;

6.4 Development with code review for releases using tools for Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST);

6.5 Vulnerability management and remediation within timelines within policy timelines;

6.6 Segregation of duties for development review and release management;

6.7 ParsePort has and will maintain a formal change management program with segregation of duties.

7 Monitoring. ParsePort will provide network, system and application monitoring including servers, disks and Security events for any potential problems designed to:

7.1 Review changes to systems and infrastructure;

7.2 Review changes which handle systems, authentication authorization and auditing;

7.3 Review privileged access to ParsePort systems;

7.4 Review access to ParsePort production environment including abnormal access; and

7.5 Engage third party vulnerability and penetration testing for ParsePort systems environment on a regular basis with a report available for Customers upon request.

8 Encryption. ParsePort will provide reasonable assurance of the protection of Customer’s data through encryption algorithms, which includes:

8.1 Transmission encryption using SHA 256 with minimum TLS 1.2;

8.2 Encryption at rest using AES 256; and

8.3 Full disk encryption on all hard drives with access to production data with AES 256.

9 Incident Response. ParsePort will maintain an incident response policy with procedures to provide Customer with reasonable assurances that ParsePort can respond to any type of security event or breach, and which includes:

9.1 Roles and responsibilities with a team and a dedicated leader which is tested annually;

9.2 Methods for investigation and escalation assessing the event to determine the risk the event poses including proper escalation;

9.3 Processes regarding internal communications, reporting and notification and external reporting and notification to customers without undue delay, and in any case, where feasible, notify within forty-eight (48) hours of an occurrence, discovered by ParsePort and not solely and directly caused by the Customer, that actually or imminently jeopardizes, without lawful authority, the integrity or confidentiality of Customer's data or the availability of ParsePort' Services (to facilitate timely notification Customer must register and maintain an up-to-date email with notice to security@parseport.com; where no such email is provided, Customer acknowledges that the means of notification shall be at ParsePort's reasonable discretion);

9.4 Appropriate documentation of the event, incident, and investigation of what was done and by whom with authorization for later analysis and possible legal action; and

9.5 An audit of the incident conducting root cause analysis and remediation.

10 Contingency Planning. ParsePort will maintain policies and procedures for the response and or recovery of an emergency or other occurrence either natural or pandemic that could damage or affect systems, and the environment of Customer's data. Such procedures include:

10.1 Data resiliency through redundancy to recover data;

10.2 Regular data backups, including annual testing of the backup and restoration procedures;

10.3 Business Continuity and Disaster Recovery plan which is communicated and made available within an event to minimize the impact and or loss of vital resources;

10.4 Annual testing of the Business Continuity Plan and Disaster Recovery Plan (Executive Summary available to Customer upon request); and

10.5 Auditing of the Disaster Recovery test.

11 Audit and Testing.

11.1 So that Customer can verify ParsePort's compliance with the DPA, upon Customer's request, ParsePort shall provide to Customer (at its ParsePort's expense) the following: (a) Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ); (b) ISAE3402 Type II; and (f) Penetration Testing of ParsePort equivalent, non-production environment which includes: (i) network scanning; (ii) improper input handling (e.g., cross site scripting, SQL injections, XML injection, and cross site flashing); (iii) weak session management; (iv) insufficient authentication; (v) insufficient authorization; (vi) data validation flaws and data integrity; (vii) OWASP Top 10; and (viii) CWE/SANS Top 25 (collectively, the "Reports").

11.2 If Customer reasonably demonstrates that the Reports provided are insufficient to demonstrate ParsePort's compliance with the DPA or the Security Standards, at Customer's expense ParsePort shall also provide written responses (on a confidential basis) to reasonable requests for information related to ParsePort's processing or security of customer data, including responses to information security and audit questionnaires, no more than once in any twelve (12) month period.

11.3 If Customer reasonably demonstrates that the information provided pursuant to Sections 11.1 and 11.2 is insufficient to demonstrate compliance with the DPA or the Security Standards, subject to Section 11.4, Customer may perform at Customer's expense:

(a) An audit in relation to ParsePort's processing and security of customer data (which may also be performed by Customer's third-party auditor, subject to ParsePort's reasonable approval) ("Audit"); or

(b) A penetration test of an equivalent, non-production environment, subject to ParsePort's reasonable approval) ("Pen Test ").

11.4 Following receipt by ParsePort of a request arising out of 11.3(a) or 11.3(b), ParsePort and Customer shall mutually agree in advance on details of such Audit or Pen Test, including the start date, scope and duration, as well as reasonable conditions designed to mitigate potential risks to confidentiality, security, or other potential disruption of the Services or ParsePort's business. Audits, Pen Tests, and any information arising therefrom are deemed ParsePort's Confidential Information. If Customer discovers any actual or potential vulnerability in connection with a Pen Test, Customer must immediately disclose it to ParsePort and shall not disclose it to any third-party. Customer shall immediately notify ParsePort with information regarding any material noncompliance discovered during the course of an Audit. Customer acknowledges that Audits and Pen Tests will be performed at Customer's own expense, with thirty (30) days advance written notice to ParsePort, during normal business hours (unless otherwise mutually agreed upon in advance for Pen Tests), no more than once in any twelve (12) month period, subject to ParsePort’s reasonable security and confidentiality requirements, and solely to the extent the exercise of rights under Section 11.3 would not infringe applicable data protection laws.

12 Disposal. ParsePort has policies and procedures to provide reasonable assurance to the appropriate disposal of Customer’s data including:

12.1 Secure shredding of printed documents and Customer’s data; and

12.2 Secure destruction of Customer Data with a certificate of destruction provided by ParsePort.

13 Endpoint Devices. ParsePort has policies, procedures, and technical controls to protect endpoint devices including:

13.1 Malware protection with automated updates and centralized tracking and management, and regular updates and patches;

13.2 Full Disk Encryption (mitigating control as Customer’s data is not stored on endpoint devices);

13.3 Regular updates and patching of the Subscription Services, ParsePort's systems and browsers; and

13.4 No use of removable media (USB).

14 Malware and Patching. Throughout the Agreement Term and in accordance with standard industry practice, ParsePort will:

14.1 Perform regular monitoring for security patches;

14.2 Apply patches in a timely manner after testing through change control; and

14.3 Regularly update systems and networks with new releases.

15 Shared Security Model.

15.1 Customer acknowledges the security of the Products and Services is a shared responsibility between ParsePort and Customer. Accordingly, Customer will administer controls as recommended by commercially reasonable security frameworks (e.g., NIST, ISO, ParsePort's security recommendations). Security regarding usage within the Product is the responsibility of the Customer. Technical security, as outlined in these requirements, is the responsibility of ParsePort. Customer shall promptly report to ParsePort any suspicious activities related to Customer’s accounts and usage (e.g., a user credential has been compromised).